Period and autocorrelation of some pseudo chaotic sequences with LSB extension by m-sequences

Hyojeong Choi, Sangwon Chae, Daekyeong Kim, Hong-Yeop Song
School of Electrical and Electronic Engineering
Yonsei University
Seoul, Korea
{hjchoi3022, sw.chae, daky33, hysong}@yonsei.ac.kr

Yundong Lee, Sangung Shin, Hongjun Noh
Tactical Communication Systems Waveform R&D
LIG Nex1
Gyeonggi-do, Korea
{yundong.lee, sangung.shin, hongjun.noh}@lignex1.com

***Abstract*— This paper analyzes the period and autocorrelation properties of pseudo chaotic sequences generated using the Least Significant Bit (LSB) extension method for the digital implementation of chaotic systems. For the application of the LSB extension method, we consider Bernoulli maps, Tent maps, and Chebyshev maps. We employed m-sequences for LSB extension, and we confirmed that the resulting pseudo chaotic sequences have some periodic orbits due only to the period of the m-sequence and some ideal autocorrelation properties.**

Keywords—DSSS systems, Chaotic maps, m-sequences, LSB extensions

I. Introduction

A chaotic map is a nonlinear function characterized by its sensitivity to initial values, where even slight differences in initial values can lead to completely distinct outcomes [1]. Due to this characteristic, it becomes possible to easily generate infinitely different sequences solely by varying the initial values.

In conventional Direct Sequence Spread Spectrum (DSSS) systems, PN codes with fixed periods are used, limiting the size of the sequence set. In contrast, chaotic maps can generate an infinite number of non-periodic signals, depending on initial value differences. Therefore, the use of chaotic sequences in existing DSSS systems employing PN codes has been studied [2-4, 9].

Implementing chaotic sequences in digital systems using fixed or floating-point arithmetic can lead to round-off and truncation errors [5-8]. Due to these issues, chaotic sequences generated with fixed or floating-point arithmetic tend to converge to arbitrary values or exhibit short periods. Recently, to address these digital implementation challenges and for cryptographic applications, the LSB extension method has been proposed [5-6]. These methods do not rely on fixed or floating-point arithmetic, but instead use simple logical operations like AND, OR, NOT, and so on. This approach allows them to be free from rounding errors. The LSB extension method for Binary Shift Chaotic Maps (BSCMs) proposed in [5] can generate pseudo chaotic sequences and true periodic sequences using a Pseudo Random Number Generator (PRNG). The BSCM is defined as chaotic maps where multiplications are binary shift operations and do not have overflows during additions. We should note that the LSB extension method for this BSCM is also not a true chaotic sequence because it is an arithmetic in a digital implementation with finite precision. In [5-6], Bernoulli maps, Tent maps, and Baker's maps were considered as BSCMs, and using their conjugate functions, Chebyshev maps, logistic maps, and others were implemented.

This paper analyzes the period and autocorrelation properties of pseudo chaotic sequences generated by Bernoulli maps, Tent maps, and Chebyshev maps based on the algorithm proposed in [5]. In Section II, a brief investigation of these maps and LSB extension method is conducted, and in Section III, the period and autocorrelation properties of the generated sequences are analyzed. Section IV concludes the paper with some concluding remarks.

II. some Binary Shift Chaotic Maps and LSB Extension

A. Binary Shift Chaotic Maps

First, we will consider is the *Bernoulli map* $S:[0,1)\rightarrow[0,1)$ is defined as follows :

$$S(x)=2x \pmod 1=\begin{cases}2x, & 0\le x\le 1/2\\ 2x-1, & 1/2\le x<1\end{cases} \tag{1}$$

Note that the Bernoulli map S involves only the operation of doubling x, which can be described as discarding the most significant bit and performing a left shift operation by one position. In other words, $S(.b_1\,b_2\,b_3\cdots)_2=(.b_2\,b_3\,b_4\cdots)_2$.

The second BSCM is the *Tent map* $T:[0,1]\rightarrow[0,1]$, and it is defined as follows :

$$T(x)=\begin{cases}2x, & 0\le x<1/2\\ 2(1-x), & 1/2\le x\le 1\end{cases} \tag{2}$$

The implementation of Tent map is essentially the same as the Bernoulli map, with the only difference being the application of the operation $(1 - x)$ in (2).

Finally, we consider the Chebyshev map $f:[-1,1] \rightarrow [-1,1]$ defined as follows :

$$f(x) = 8x^4 - 8x^2 + 1 \qquad (3)$$

The operation of this map can be implemented by applying the twice iterated Bernoulli map $S^2 = S \circ S$ and its conjugate function $h(x) = \cos(2\pi x)$. A detailed explanation of the conjugacy map can be found in Chapter 4 in [5].

B. LSB Extension Method

The key idea of the LSB extension method is explained in Chapter 2 in [5]. In this approach, all operations are conducted on an L-bit memory unit representing the initial L bits of binary numbers. When performing a k-bit left shift, the least significant k bits become zeros. In such cases, these zeros are replaced by random bits using a PRNG. All the BSCMs described in subsection A can be implemented by simply performing left shift operations and taking complements of the L bits in the memory unit. The implementation algorithm for LSB extension of these BSCMs is detailed in [5-6].

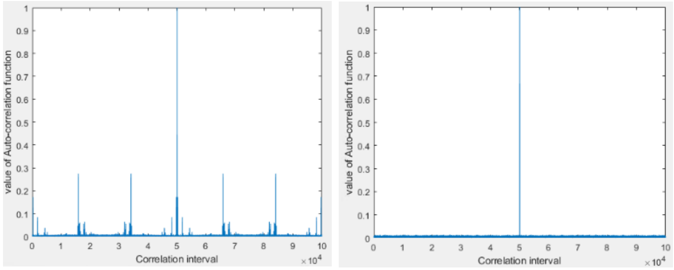
III. Period and AutoCorrelation Properties of BSCMs

In this paper, we consider output sequences of length 50,000 obtained by applying LSB extension to each BSCM. The number of memory units for all experiments is set to 16. Therefore, since the output sequences are quantized between 0 and 1 with a resolution of 2^{16}, each output value was mapped to the 2^{16}-th root of unity for autocorrelation calculations. The autocorrelation calculation formula is as follows :

$$R(\tau) = \sum_{i=0}^{N-1} x(i) \cdot x^*(i - \tau). \qquad (4)$$

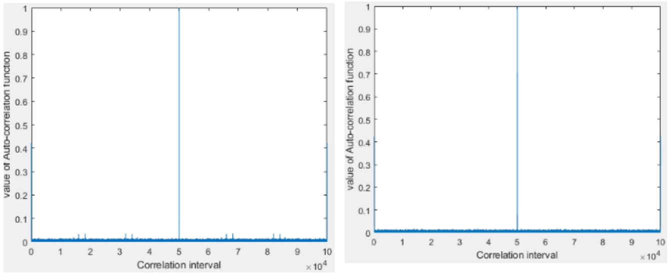
In this paper, we consider m-sequences generated by 16-bit and 32-bit LFSRs as the PRNGs used for LSB extension. Figures 1, 2, and 3 demonstrate the autocorrelation characteristics of output sequences generated through the LSB extension algorithm using Bernoulli maps, Tent maps, and Chebyshev maps as BSCMs, respectively. For all cases, the initial value of the LFSR set to have only the first bit as 1 and the rest as 0, while the initial values of the BSCMs fixed at 0.7. As can be seen in the figures, all three maps exhibit better autocorrelation characteristics when a 32-bit LFSR is applied.

In this paper, we considered sequences of length 50,000. However, in fact, both the Bernoulli map and the Chebyshev map undergo simple left shift operations, so they have the same period as the used m-sequence. Therefore, when applying m-sequences generated by a 16-bit and 32-bit LFSR for LSB extension, their respective periods become $2^{16} - 1$ and $2^{32} - 1$. On the other hand, the Tent map, in contrast, incorporates not only simple left shift operations but also a process of taking complements for L bits. Therefore, its period becomes the product of the period of the m-sequence and the number of memory units. Considering 16-bit memory units, the period of the output sequences of the Tent map, when m-sequences generated by 16-bit and 32-bit LFSRs are applied for LSB extension, becomes $2^{16} \cdot 16$ and $2^{32} \cdot 16$, respectively.



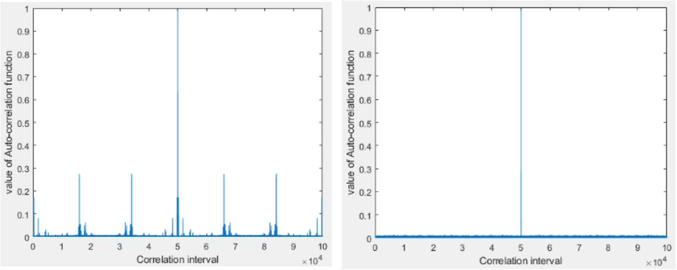
(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 1. The autocorrelation of the output sequences of *Bernoulli map*



(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 2. The autocorrelation of the output sequences of *Tent map*



(a) Using a 16-bit LFSR (b) Using a 32-bit LFSR

Fig. 3. The autocorrelation of the output sequences of *Chebyshev map*

IV. Conclusion

This paper analyzes the period and autocorrelation properties of pseudo chaotic sequences generated using the LSB extension method for the digital implementation of chaotic systems. We consider applying the LSB extension method to Bernoulli maps, Tent maps, and Chebyshev maps, using m-sequences for LSB extension. As a result, it was observed that the Tent map exhibited the longer period and better autocorrelation properties compared to the Bernoulli map and Chebyshev map under the same experimental conditions.

Acknowledgment

The This work was supported by Korea Research Institute for defense Technology planning and advancement(KRIT) grant funded by the Korea government (DAPA(Defense Acquisition Program Administration)). (No. 11-202-205-010(KRIT-CT-22-086, Aperiodic, non-predictable, randomness and denseness signaling ultra-low-probability-of-detection and covert communication technology, 2023.)

REFERENCES

[1] R. L. Devaney, *An introduction to chaotic dynamical systems*, CRC press, 2003.

[2] H. Jiang and C. Fu, “A chaos-based high quality PN sequence generator,” *International Conference on Intelligent Computation Technology and Automation*, pp. 60-64, 20–22 October 2008.

[3] T. Kohda and A. Tsuneda, “Pseudonoise sequences by chaotic nonlinear maps and their correlation properties,” *IEZCE Trans.*, vol. E76-B, no.8, pp. 855-862, 1993.

[4] F. Liu, S. Jia, X. Xu and M. Tian, “Improved Chaotic Sequence Generation Method Based on Direct Spread Spectrum.” *Journal of Physics: Conference Series*, vol. 1237, no. 4, 2019.

[5] I. Öztürk and R. Kilic, “Digitally generating true orbits of binary shift chaotic maps and their conjugates,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 62, pp. 395‐408, Sep. 2018.

[6] I. Öztürk and R. Kilic, “Utilizing true periodic orbits in chaos-based cryptography,” *Nonlinear Dynamics*, vol.103, pp. 2805-2818, 2021.

[7] C. Guyeux and J. M. Bahi, “Hash functions using chaotic iterations,” *J. Algorithms Comput. Technol.*, vol. 4, no. 2, pp. 167–182, 2010.

[8] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, “Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems,” *IEEE Trans. Circuits Syst. I*, Reg.

[9] Hyunwoo Cho, Hyojeong Choi, Daekyeong Kim, Min Ahn, and Hong-Yeop Song, “Statistical Tests of Some Binary Chaotic and Pseudorandom Sequences,” *The European Navigation Conference (ENC) 2023*, Noordwijk, Netherlands, May 31 - June 2, 2023.